Zoom Security Concerns and Advice for Parishioners

KIDDERMINSTER EAST PARISH
Five Churches One Parish One Lord

Many people are now using Zoom to keep in touch with friends and family, as well as for meetings and church services.

Over 2020, the company has added 2.2 million new monthly users, outstripping the entire 2019 new user base of 1.19 million. This massive escalation in its usage has created security ramifications. Zoom has tried to clean up its act, and quickly. To try and prevent Zoom-bombing -- the hijack of meetings, meeting ID numbers will no longer be shown in address bars. A dedicated security tab has also been introduced to streamline the process of changing security settings for hosts and meeting attendees. Zoom has also promised an upcoming change to where data is stored.

There are some actions we can take when setting up Zoom calls to help keep them as secure as possible, and to protect ourselves and our audience, which we would like to share with you:

1. PASSWORD PROTECT YOUR MEETINGS

The simplest way to prevent unwanted attendees and hijacking is to set a password for your meeting. Passwords can be set at the individual meeting, user, group, or account level for all sessions. In order to do so, first sign in with your account at the Zoom web portal. If you want to set up a password at the individual meeting level, head straight over to the "Settings" tab and enable "Require a password when scheduling new meetings", which will ensure a password will be generated when a meeting is scheduled. All participants require the password to join the meeting. (Subscription holders can also choose to go into "Group Management" to require that everyone follows the same password practices.)

2. ENSURE THE PASSWORD IS NOT EMBEDDED IN THE MEETING LINK

There is a setting in Zoom which allows passwords to be embedded in the meeting link and therefore attendees do not have to enter the password to gain access.
For added security, to ensure that the password is required to access a meeting, the host should turn off the "Embed password in invite link for one-click join" - to do this please logon to the Zoom website, go to "Settings", ensure "Meeting" is selected and scroll down to the "Embed Password" option to ensure that it is turned off. This action should be done prior to creating the meeting and will apply to all meetings going forward unless you turn the setting back on.

2. AUTHENTICATE USERS

When creating a new event, you should choose to only allow signed-in users to participate.

3. JOIN BEFORE HOST

Do not allow others to join a meeting before you, as the host, have arrived. You can enforce this setting for a group under "Account Settings."

4. TURN OFF PARTICIPANT SCREEN SHARING

No-one wants to see pornographic material shared by a Zoom bomber, and so disabling the ability for meeting attendees to share their screens is worthwhile. This option can be accessed from the new "Security" tab in active sessions.

5. USE A RANDOMLY-GENERATED ID

You should not use your personal meeting ID if possible, as this could pave the way for pranksters or attackers that know it to disrupt online sessions. Instead, choose a randomly generated ID for meetings when creating a new event. In addition, you should not share your personal ID publicly.

6. USE WAITING ROOMS

The Waiting Room feature is a way to screen participants before they are allowed to enter a meeting. While legitimately useful for purposes including interviews or virtual office hours, this also gives hosts greater control over session security.

7. AVOID FILE SHARING

Be careful with the file-sharing feature of meetings, especially if users that you don't recognize are sending content across, as it may be malicious. Instead, share material using a trusted service such as Box or Google Drive. At the time of writing, Zoom has disabled this feature anyway due to a "potential security vulnerability."

8. REMOVE NUISANCE ATTENDEES

If you find that someone is disrupting a meeting, you can kick them out under the "Participants" tab. Hover over the name, click "More," and remove them. You can also make sure they cannot rejoin by disabling "Allow Removed Participants to Rejoin" under the "Settings: Meetings - Basic" tab.

9. CHECK FOR UPDATES

As security issues crop up and patches are deployed or functions are disabled, you should make sure you have the latest build. In order to check, open the desktop application, click on your profile in the top-right, and select "Check for updates."

Another way we can receive intrusions is via phishing emails. Please see this article relating to Zoom in particular:
https://www.forbes.com/zooms-200-million-users-are-facing-a-new-threat-heres-what-to-do

PARISH PROTOCOL

In order to keep security for “meetings” as tight as possible, and yet involve all who wish to join in, if you are setting up a Zoom call which is an open meeting for others in the parish to join, please would you send the Zoom login details, including the password, to: parishcomms@kidderminstereast.org.uk You should also ask those who wish to participate to register their interest in that service / meeting, via the same email address, at least 24 hours in advance. The meeting link, ID and Password will then be shared with all the participants via Mailchimp. This is good practice and is recommended for everyone’s security.

If, however, you are running a meeting for a small, private group (e.g. homegroup) there is no need to share the login details in this way. The details can be sent directly to multiple participants via email, respecting their preferences for data sharing by bcc‘ing, where applicable.

If you wish your service / meeting to be advertised parish-wide, please also send a notice to be included in the weekly newsletter, if possible by the Wednesday prior to the newsletter being published, to: office@kidderminstereast.org.uk